

1 NICOLA T. HANNA
United States Attorney
2 BRANDON D. FOX
Assistant United States Attorney
3 Criminal Division
JENNIFER CHOU (Cal. Bar No. 238142)
4 Assistant United States Attorney
Violent & Organized Crime Section
5 1300 United States Courthouse
312 North Spring Street
6 Los Angeles, California 90012
Telephone: (213) 894-6482
7 Facsimile: (213) 894-3713
Email: jennifer.chou@usdoj.gov
8

Attorneys for Applicant
9 UNITED STATES OF AMERICA

10 UNITED STATES DISTRICT COURT

11 FOR THE CENTRAL DISTRICT OF CALIFORNIA

12 IN THE MATTER OF THE SEARCH OF:
INFORMATION ASSOCIATED WITH
13 ACCOUNT IDENTIFIED AS
MIKEBATZPHOTOGRAPHY.SMUGMUG.COM
14 THAT IS STORED AT THE PREMISES
CONTROLLED BY SMUGMUG, INC., 67
15 E. EVELYN AVENUE, SUITE 200,
MOUNTAIN VIEW, CA 94041
16

No. 19-MJ-00258

GOVERNMENT'S EX PARTE APPLICATION
FOR FIRST EXTENSION OF TIME WITHIN
WHICH TO RETAIN AND SEARCH DIGITAL
DEVICES; DECLARATION OF JENNIFER
CHOU

(UNDER SEAL)

17
18 The United States of America, by and through its counsel of
19 record, Assistant United States Attorney Jennifer Chou, hereby
20 applies for an order extending, nunc pro tunc, by 120 days the time
21 within which the government may retain and search digital devices
22 seized pursuant to a federal search warrant, specifically, to
23 November 22, 2019.

24 //

25 //

26 //

27 //

28

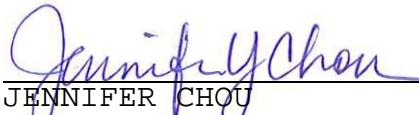
1 This application is based on the attached declaration of
2 Jennifer Chou and the files and records of this case, including the
3 underlying search warrant and affidavit in support thereof.

4 Dated: July 25, 2019

Respectfully submitted,

5 NICOLA T. HANNA
United States Attorney

6
7 BRANDON D. FOX
Assistant United States Attorney
Chief, Criminal Division

8
9 
10 JENNIFER CHOU
Assistant United States Attorney

11 Attorneys for Applicant
12 UNITED STATES OF AMERICA
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DECLARATION OF JENNIFER CHOU

I, Jennifer Chou, hereby declare and state:

1. I am an Assistant United States Attorney assigned to this investigation for United States Attorney's Office for the Central District of California. I am familiar with this investigation and have learned the following information from the case agent, Federal Bureau of Investigation ("FBI") Special Agent ("SA") Emily Tripp.

2. This declaration is made in support of a request for a nunc pro tunc¹ order permitting the government to retain and search, pursuant to the terms of the original warrants in this matter, for an additional 120 days, the response received from SmugMug, Inc. ("SmugMug") seized pursuant to the warrant described below (the "SUBJECT DATA").

3. On January 31, 2019, SA Tripp obtained federal search warrant No. 19-258M, issued by the Honorable Paul L. Abrams, United States Magistrate Judge, authorizing the search of information associated with the account identified as "mikebatzphotography.smugmug.com" (the "SmugMug account") that is stored at the premises controlled by SmugMug at 67 East Evelyn Avenue, Suite 200, in Mountain View, California 94041 (the "SUBJECT DATA"). The warrant, which is attached at Exhibit A and incorporated herein by reference, authorized the search of the SUBJECT DATA for a period of 120 days from the date of the FBI's receipt of SmugMug's response to allow the government to search such devices for evidence of violations of 18 U.S.C. § 2251 (a), (e), attempted production of

¹ As discussed below, the government inadvertently delayed filing this request until after the applicable deadlines to complete the search of the seized digital devices expired.

1 child pornography; 18 U.S.C. § 2252A(a)(2)(A), (b)(1), attempted
2 receipt of child pornography; and 18 U.S.C. § 2433(b), enticement.

3 4. On February 4, 2019, SA Emily Tripp served the warrant to
4 SmugMug via email and received the SUBJECT DATA from SmugMug on
5 February 11, 2019. Accordingly, the end of the authorized 120-day
6 search period was June 11, 2019.

7 5. The data contained in the SUBJECT DATA from SmugMug was
8 voluminous and provided in a secured format that required the FBI to
9 spend additional time to gain access. On or about February 22, 2019,
10 SA Tripp was able to access the files and begin the process of
11 extracting and unzipping the SUBJECT DATA files for review. On March
12 12, 2019, SA Tripp completed the access process and was finally able
13 to view the SUBJECT DATA files.

14 6. On March 13, 2019, SA Tripp began a preliminary review of
15 the SUBJECT DATA files and determined that the SUBJECT DATA files
16 contain over 97,500 images, over 1,000 videos, and over 100,500
17 files.

18 7. In her preliminary review, SA Tripp observed evidence of
19 suspected child pornography, including videos and images that
20 depicted young females, both known and unknown to law enforcement,
21 engaged in sexual activity with the user of the SmugMug account,
22 Miguel Angel Batz, Jr. ("BATZ").

23 8. SA Tripp continued to review the SUBJECT DATA until on or
24 about June 3, 2019, at which point she shifted her attention to
25 reviewing voluminous extraction data from several of BATZ's digital
26 devices. She did not complete her review of the SUBJECT DATA.

27 9. Through an oversight, and because she was primarily focused
28 on her review of the digital device extraction data, SA Tripp failed

1 to seek an extension before June 11, 2019, for the SUBJECT DATA. She
2 realized her oversight on or about July 1, 2019.

3 10. Law enforcement has not reviewed the SUBJECT DATA since
4 June 3, 2019.

5 11. For the following reasons, the government is requesting,
6 nunc pro tunc, an additional 164 days, to November 22, 2019, to
7 complete its review of certain of the content records:

8 a. The SUBJECT DATA contains approximately 694 gigabytes
9 of information. Based on her training and experience, SA Tripp knows
10 that one gigabyte could hold the contents of about ten yards of books
11 on a shelf. One hundred gigabytes could hold an entire library floor
12 of academic journals.

13 b. SA Tripp also maintains other work obligations, such
14 as participating on a Task Force with the Los Angeles Police
15 Department and the Los Angeles Sheriff's Department Human Trafficking
16 Units, responds to time sensitive call-outs for juvenile sex
17 trafficking investigations, and maintains investigative and
18 administrative obligations to other crimes against children cases.
19 Additionally, she is the coordinator for a national human trafficking
20 operation that is being conducted throughout July 2019.

21 //

22 //

23 //

EXHIBIT A

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of:)
Information associated with account identified as) Case No. 2:19-MJ-00258
mikebatzphotography.smugmug.com that is stored at)
premises controlled by SmugMug, Inc., 67 E. Evelyn)
Avenue, Suite 200, Mountain View, CA 94041)

WARRANT PURSUANT TO 18 U.S.C. § 2703

To: Any Authorized Law Enforcement Officer

An application by a federal law enforcement officer requests the production and search of the following data:

See Attachment A

The data to be produced and searched, described above, are believed to contain the following:

See Attachment B

I find that the affidavit, or any recorded testimony, establishes probable cause to produce and search the data described in Attachment A, and to seize the data described in Attachment B. Such affidavit is incorporated herein by reference.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE HEREBY COMMANDED to serve this warrant on SmugMug, Inc. in the daytime, between the hours of 6:00 a.m. and 10:00 p.m., within 14 days from the date of its issuance.**SMUGMUG, INC. IS HEREBY COMMANDED** to produce the information described in Attachment A within 10 calendar days of the date of service of this order. **SMUGMUG, INC. IS FURTHER COMMANDED** to comply with the further orders set forth in Attachment B, and, pursuant to 18 U.S.C. § 2705(b), shall not notify any person, including the subscriber(s) of the account/s identified in Attachment A, of the existence of this warrant.

The officer executing this warrant, or an officer present during the execution, shall prepare an inventory as required by law, and shall promptly return this warrant and the inventory to the United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

AUTHORIZED LAW ENFORCEMENT OFFICER/S IS/ARE FURTHER COMMANDED to perform the search of the data provided by **SMUGMUG, INC.** pursuant to the procedures set forth in Attachment B.

Date and time issued: JAN 31 2019 1:00p.m.

PAUL L. ABRAMS

Judge's signature

City and State: Los Angeles, CA

Hon. Paul Abrams, U.S. Magistrate Judge

Printed name and title

Return*Case No:**Date and time warrant served on provider:**Inventory made in the presence of:**Inventory of data seized:*

[Please provide a description of the information produced.]

Certification

I declare under penalty of perjury that I am an officer involved in the execution of this warrant, and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the account identified as mikebatzphotography.smugmug.com that is within the possession, custody, or control of SmugMug, Inc. (the "PROVIDER"), a company that accepts service of legal process at 67 E. Evelyn Avenue, Suite 200, Mountain View, CA 94041, regardless of where such information is stored, held, or maintained.

ATTACHMENT B

ITEMS TO BE SEIZED

I. SEARCH PROCEDURE

1. The warrant will be presented to personnel of SmugMug, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a. below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other

sophisticated techniques, including to search for known images of child pornography.

5. If the search team encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 120 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the content records beyond this 120-day period without first obtaining an extension of time order from the Court.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT, limited to that which occurred on or after April 2013, which is three months before the first text message indicating that BATZ may be involved in the production of child pornography,⁵ including:

i. All e-mails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the account, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information

⁵ To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

associated with each e-mail or message, and any related documents or attachments.

ii. All records or other information stored, sent, or received by subscriber(s) of the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All folders and files associated with the SUBJECT ACCOUNT, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, the date and time at which each file was sent, and any user-created organizational structure within the SUBJECT ACCOUNT.

iv. All transactional information of all activity of the SUBJECT ACCOUNT described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting, and emails "invites" sent or received via SmugMug, and any contact lists.

v. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's

full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

(I) the SUBJECT ACCOUNT.

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Section II.10.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made, any and all logs of user activity and user agent string, including: web requests or HTTP requests; any logs containing information such as the Requestor's IP address, identity and user ID, date and timestamp, request URI or URL, HTTP protocol version, referrer, and other user agent string information; login tracker logs;

account management logs; and any other information concerning other e-mail or social media accounts accessed by or analytics related to the SUBJECT ACCOUNT; any and all cookies used by any computer or web browser associated with the SUBJECT ACCOUNT, including the IP addresses, dates, and times associated with the recognition of any such cookie.

(I) any other account associated with the cookie(s) associated with the SUBJECT ACCOUNT.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT ACCOUNT listed in Attachment A, the search team may seize:

a. All information described above in Section II.10.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2251 Sexual Exploitation of Children and 18 U.S.C. §§ 2252A(a)(1), (5)(B) Distribution and Possession of Child Pornography, namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNT, including records about their identities and whereabouts.

ii. Any files or records that refer to or depict child pornography, as defined in 18 U.S.C. § 2256(8), or the sexual exploitation of children, including but not limited to documents that refer to the possession, receipt, distribution, production, transmission, reproduction, viewing, sharing, purchasing, downloading, shipment, order, requesting, trade, soliciting, or transaction of any kind, involving child pornography or the sexual exploitation of children.

iii. Any files, records, pictures, or videos tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256.

iv. Any files or records that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

v. Any and all files or records which are sexually arousing to individuals who are interested in minors. Such material is commonly known as "child erotica" and includes images of children, written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

vi. Any files or records that pertain to accounts with any Internet Service Provider.

vii. Any passwords, encryption keys, and other access devices that may be necessary to access folders and files in the SUBJECT ACCOUNT;

viii. Any communications, files, records, photos, or videos referring to or depicting the solicitation of nude or partially nude images from individuals who may be minors;

ix. Any nude or partially nude images or videos of individuals who may be minors;

x. Any communications, files, records, photos, or videos referring to or depicting the solicitation of sex or sexual acts from individuals who may be minors, including soliciting sex in exchange for money, drug, goods, favors, or any other reason;

xi. Any communications, files, records, photos, or videos referring to or depicting the solicitation of sex or sexual acts from individuals who may be minors;

xii. Any communications, files, records, photos, or videos referring to or depicting sex or sexual acts involving an individual who may be a minor;

b. All records and information described above in Section II.10.b.

IV. PROVIDER PROCEDURES

12. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the provider shall disclose responsive data by sending it to the following address via US Mail, or to the following email address:

SA Emily Tripp
11000 Wilshire Blvd, Suite 1700
Los Angeles, CA 90024
Office Telephone: 310-996-4235
Office Fax: 310-996-4009
Email: etripp@fbi.gov

13. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

AFFIDAVIT

I, Emily Tripp, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since March 2016. I am currently assigned to the Los Angeles Field Office where I have been working on the Violent Crimes Against Children Squad since August 2016. I am also assigned to the multi-agency child exploitation task force known as the Southern California Regional Sexual Assault Felony Enforcement ("SAFE") Team, as well as the Los Angeles Innocence Lost Task Force. The SAFE Team is responsible for enforcing federal criminal statutes involving the sexual exploitation of children under Title 18, United States Code, Section 2251, et seq. I have participated in investigations into child exploitation, child pornography, and sex trafficking involving minors, and I have executed search warrants as part of those investigations. Many of the child exploitation-related investigations have involved the search, processing, and review of electronic and digital devices, including computers. I have received both formal and informal training from the FBI regarding computer-related investigations and computer technology. My formal training includes 21 weeks of formal education at the FBI Academy, where I took classes on writing affidavits and providing evidentiary testimony. I have also received training on the investigation of commercial sexual exploitation of children and juvenile sex trafficking. I have participated in the execution of numerous operations for the

rescue of juvenile victims of human trafficking. During my career as an SA with the FBI, I have participated in numerous investigations involving the sexual exploitation of children facilitated by the use of computers and other electronic devices. Prior to my employment as a SA with the FBI, I was employed as a Child Protective Services Investigator for the Department of Family and Protective Services with the state of Texas. Through both my training and experience, I have become familiar with the methods of operation used by people who commit offenses involving the sexual exploitation of children, and how people use the Internet to commit crimes arising from, and related to, the sexual exploitation of children.

2. I make this affidavit in support of an application for a warrant for information associated with the SmugMug account identified by the account name: mikebatzphotography.SmugMug.com (the "SUBJECT ACCOUNT") that is stored at premises controlled by SmugMug, Inc. (the "PROVIDER"), a provider of electronic communication and remote computing services, headquartered at 67 E. Evelyn Avenue, Suite 200, Mountain View, CA 94041.¹ The

¹ Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in

information to be searched is described in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)² to require the PROVIDER to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B. Attachments A and B are incorporated herein by reference.

3. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with a SUBJECT ACCOUNT constitutes evidence, contraband, fruits, or instrumentalities of criminal violations

which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

² The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which does not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content (see Attachment B paragraph II.10.a.) as well as subscriber records and other records and information that do not contain content (see Attachment B paragraph II.10.b.).

of 18 U.S.C. § 2251 Sexual Exploitation of Children and 18 U.S.C. §§ 2252A(a)(1), (5)(B) Distribution and Possession of Child Pornography.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents, witnesses, and evidence that members of the investigation have reviewed. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF INVESTIGATION

5. In or around March 2018, law enforcement began investigating a complaint that MIGUEL ANGEL BATZ, JR. ("BATZ") had traded drugs for sexual acts with a minor. Law enforcement interviewed Minor Victim 1 ("MV1") who told law enforcement that BATZ took nude pictures of MV1 when MV1 was 17 years old, and exchanged money and drugs for sex acts even after MV1 told BATZ that MV1 was under 18 years old.

6. On or about May 24, 2018, law enforcement executed a state search and arrest warrant for BATZ and his home and found at least 20 digital devices. I also participated in an interview of BATZ on or about May 24, 2018. On June 20, 2018, I obtained a federal search warrant from the Honorable Patrick J. Walsh, case number 2:18-mj-0192, to search 20 digital devices,

including an iPhone A1549 (the "iPhone") which was in BATZ's possession at the time of his arrest on May 24, 2018. This digital device search warrant is attached hereto as exhibit A and incorporated by reference.

7. On the iPhone, I saw that BATZ and Minor Victim 2 ("MV2") exchanged text messages regarding the price of nude photographs, and referenced the fact that BATZ knew MV2 was not yet 18 years old. The iPhone also contained at least three nude pictures of MV2. In January 2014, BATZ sent text messages to MV2 indicating that BATZ had uploaded MV2's photos to the SUBJECT ACCOUNT.

8. On the iPhone, I saw that the SmugMug application was installed. Using the iPhone, while the iPhone was disconnected from the internet, I could see that local data associated with the SUBJECT ACCOUNT stored on the iPhone included image galleries named after suspected minor victims. For example, fifteen of the locally stored SmugMug galleries associated with the SUBJECT ACCOUNT included the picture and name of Minor Victim 3 ("MV3").

9. Separate from the data associated with the SUBJECT ACCOUNT, the iPhone also contained a video of MV3 having oral sex with a man who I believe to be BATZ. MV3 wore the same outfit in the iPhone video as MV3 wore in a locally stored SmugMug photo associated with the SUBJECT ACCOUNT. I believe the man in the iPhone video performing sex acts with MV3 was BATZ based on my interview with MV3. I also know that MV3 was

17 years old at the time this iPhone video was created because MV3 was still a minor when law enforcement obtained the video.

10. I believe there is probable cause that the SUBJECT ACCOUNT has additional depictions of child pornography and contains evidence that this child pornography was being produced, possessed, and possibly distributed.

III. STATEMENT OF PROBABLE CAUSE

A. LAPD Investigates and Arrests BATZ

11. On or around April 4, 2018, Los Angeles Police Department ("LAPD") Detective Sammy Cruz provide me with a police report which stated that MV1 had met BATZ in 2014. In 2014, BATZ was approximately 32 years old. According to the report, in 2017 BATZ began giving MV1 drugs in exchange for sexual acts. MV1 was a minor at the time.

12. On or about March 27, 2018, LAPD detectives conducted a recorded interview with MV1, which I have reviewed. During the interview, MV1 stated MV1 had met BATZ, and BATZ told MV1 that BATZ was a photographer. BATZ told MV1 that he would give MV1 money if MV1 sent him nude images of MV1. MV1 told BATZ that MV1 was 17 years old and he stated he knew how old MV1 was, and continued to ask for the nude pictures. MV1 sent BATZ nude pictures in exchange for money. Later, BATZ met MV1 in person to exchange money for sex acts while MV1 was still a minor.

13. MV1 identified BATZ's Instagram name to law enforcement and provided law enforcement with permission to search MV1's cell phone. On April 2, 2018, law enforcement searched MV1's cell phone and discovered an Instagram direct

message chat conversations on or around December 5, 2017, where BATZ offered to pay MV1 for nude videos. BATZ directed MV1 on what he wants in the videos and how much he will pay. On or around December 10, 2017, MV1 sent BATZ an Instagram message where she told BATZ that she was 17 years old. BATZ responded, in part, "I assumed you were cause of the age you were when we first shot. I'm fine with it." MV1 told law enforcement that she met up with BATZ to perform sexual acts in December 2017, and February 2018.

14. On May 24, 2018, I was present when LAPD executed a search and arrest warrant for BATZ and his residence. LAPD seized at least 20 digital devices, including the iPhone which was on BATZ's person. BATZ was arrested for a violation of California Penal Code Section 288a(b)(1), Oral Copulation of a Minor. I was also present at an interview with BATZ and can recognize his voice.

15. On June 20, 2018, the Honorable Patrick J. Walsh signed a federal search warrant to search the 20 digital devices, including the iPhone. This search warrant is attached hereto as Exhibit A, and is incorporated by reference. This search warrant authorized a search of, among other things, data, photographs, videos, and applications stored on the iPhone. On or about October 17, 2018, law enforcement obtained an extension of time to search the iPhone.

B. BATZ's iPhone Contains Messages About Child Exploitation

16. In or about November 2018, I searched the files and data locally stored on the iPhone. At the time of the search, the iPhone was disconnected from the internet and could not access any outside servers. During this search, I discovered that the iPhone had the SmugMug application³ installed. As discussed in further detail below, SmugMug and the SUBJECT ACCOUNT on SmugMug were referenced in BATZ's conversations with MV2.

17. In the iPhone, I found and reviewed text messages between BATZ and MV2, including the following exchange:

a. On or around November 10, 2013 BATZ and MV2 discussed arranging a "one on one" photo shoot, and asking if MV2 is willing to do full nude photos "like last time." MV2 responded that MV2 would do full nude photos for the same price as last time, \$150 for the last hour, or just topless photos for \$90.

18. In the iPhone, I found three pictures of MV2 nude seated on a couch facing the camera with MV2's vaginal area exposed. Based on the metadata in these pictures, these pictures were taken in or about July 2013.

19. Through further investigation, I discovered MV2's identity and obtained MV2's California Department of Motor Vehicles ("DMV") records. Through these records I confirmed

³ SmugMug is a photo gallery application, mainly used by photographers, to securely store, share, or sell photographs to others.

that MV2 was 17 years old on November 10, 2013. I also obtained MV2's DMV photo and visually confirmed that MV2 was the person in the three nude iPhone pictures.

20. On November 11, 2013, BATZ texted MV2 and wrote, "Hey when you turn 18 are you gonna publicly post your topless pics? If you plan to, I will hold on to the ones we shot yesterday and edit them for you when you turn 18 cause there's a couple that are really artistic looking in black and white."

21. On or about December 5, 2013, BATZ offered MV2 \$125 plus marijuana for a nude photo shoot. MV2 agreed but stated "im not like spreading my lips or anything just artistic nude." BATZ replied, "but that's what I wanted, you used to send me some sexy pics I wanted to shoot some of my own."

22. On or about January 26, 2014, BATZ sent MV2 a text message saying that he had completed editing MV2's photos and he will upload them to SmugMug. On or around January 31, 2014, BATZ sent MV2 a link to the SUBJECT ACCOUNT.

23. In the iPhone, I also discovered numerous text messages to different people which included links to the SUBJECT ACCOUNT. I noticed that typically the SUBJECT ACCOUNT links were for galleries which match the name of the women in the text messages. I have not yet identified all of these individuals or whether they were all minors when the pictures were taken.

24. On November 6, 2018, I reviewed the locally stored data associated with the SmugMug application on the iPhone. The iPhone was not connected to the internet or any outside servers when I was reviewing this data. Thus, when reviewing this data,

I was only able to view locally stored data on the iPhone. Meaning I could only see the content from the SUBJECT ACCOUNT which was downloaded to the iPhone and available when not connected to the internet. I was unable to view the portion of the SUBJECT ACCOUNT which was not downloaded onto the iPhone. To view the remaining portion of the SUBJECT ACCOUNT, this search warrant is necessary.

25. In my review, I saw that the SUBJECT ACCOUNT contained multiple galleries bearing different female names. Each gallery had a picture of a woman I believe BATZ had photographed and uploaded, based on text message conversations corresponding to the names of some of the galleries. Some of the females in the gallery profile pictures were nearly nude, nude, topless, or bottomless. I have confirmed that at least one of the women, MV3, depicted in these galleries was a minor.

26. Approximately 15 galleries in the SUBJECT ACCOUNT bore a picture of MV3. One of the galleries with MV3's name was marked private. The private gallery had a profile picture of MV3 in a white t-shirt cut to expose the abdomen and lower portion of her breasts and black thong underwear. I recognized the pictures on the SUBJECT ACCOUNT as matching pictures saved in the iPhone where MV3 was wearing what appeared to be the same outfit. The metadata for the matching picture on the iPhone indicated that the photos were taken on April 22, 2018.

27. The iPhone also contained a series videos of MV3 in the same white t-shirt and black thong where MV3 appears to be

performing sexual acts on BATZ. These videos were stored separately from the SmugMug application on the iPhone.

28. In one of these videos, MV3 is nude and appears to manually stimulating BATZ's erect penis. In the video, the man sounds like BATZ and asks MV3 why MV3 has oral sex with other "random guys." MV3 replied that she is upset because BATZ had given more money to the girl BATZ "got in trouble with."⁴ BATZ replied that he had given MV1 the "first time rate" which he had also given to MV3. In the next video, MV3 can be seen orally copulating a man's penis. The metadata for both videos indicate that they were filmed on or around April 22, 2018.

29. On December 20, 2018, I spoke to MV3 and confirmed that she was still 17 years old in May 2018, when law enforcement obtained BATZ's phone. MV3 also admitted that she had performed sexual acts with BATZ, and that BATZ had filmed her.

30. A 90-day preservation letter was sent for the SUBJECT ACCOUNT on November 7, 2018 pursuant to 18 U.S.C. § 2703(f). Therefore, I believe there is probable cause that the SUBJECT ACCOUNT contains evidence of criminal activity, in violation of 18 U.S.C. § 2251 Sexual Exploitation of Children and 18 U.S.C. §§ 2252A(a)(1), (5)(B) Distribution and Possession of Child Pornography.

⁴ Based on the context of this video, and previous text conversations between BATZ and MV3, I believe MV3 is referencing BATZ's arrangement with MV1.

31. Other than what has been described herein, to my knowledge the United States has not attempted to obtain the contents of the SUBJECT ACCOUNT by other means.

IV. BACKGROUND ON CLOUD SERVICES, E-MAIL, SOCIAL MEDIA ACCOUNTS AND THE PROVIDER

28. In my training and experience, I have learned that providers of e-mail and social media services offer a variety of online services to the public. Providers, like the PROVIDER, allow subscribers to obtain accounts like the SUBJECT ACCOUNT. Subscribers obtain an account by registering with the provider. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. I have learned that there are numerous cloud-based storage services available for consumers offering many different capabilities. In general, cloud-based storage services can be defined as an online storage medium on the Internet accessed from a computer or electronic storage device. Providers, such as SmugMug, Inc., make it possible for the user to have access to saved files, data, programs, etcetera (referred to as "contents") without the requirement of storing said contents on their own computers or other electronic storage devices; to include physical hard drives, USB drives, CDS, DVDS, etc. The PROVIDER provides an "offsite" storage medium for contents that can be viewed at any time from any device capable of accessing the Internet.

29. Users can store their contents on a cloud-based storage and avoid having the contents accessed and, in some

cases, appear on their computers. Anyone conducting a search of an individual's computer would not be able to see the contents if the user opted to store the contents in the "cloud." These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

30. In my training and experience, I know that users of cloud-based storage like the PROVIDER can access and sometimes locally store contents also stored by the PROVIDER. Often, when contents are locally stored on a device by a user, the user can access that locally stored content even when offline or without any access to any network.

31. In my training and experience, the subscriber information collected by the PROVIDER during the account registration process - such as name, address, telephone numbers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number) - may constitute evidence of crimes under investigation because the information can identify the user(s) of the SUBJECT ACCOUNT.

32. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other e-mail addresses or phone numbers supplied in

subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

32. Therefore, the computers of the PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, e-mail or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

33. A subscriber of the PROVIDER can also store with the PROVIDER files in addition other messages, such as address books, contact or buddy lists, calendar data, pictures or videos (other than ones attached to e-mails), notes, and other files, on servers maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an account may be found in such information.

34. In my training and experience, e-mail and social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or

closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a SUBJECT ACCOUNT.

35. In my training and experience, e-mail and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of e-mails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

36. I request that the PROVIDER provide the entire contents for the SUBJECT ACCOUNT since inception until the time the requested warrant is served on them, and that the items to be seized set forth in detail in Attachment B permit law enforcement to seize such items without limit as to time in

order to assist in identifying the individual(s) participating in the possession, receipt, distribution, and production of child pornography. I further request this because the SUBJECT ACCOUNT may have historical information about the identities of the user(s) of one or other accounts involved in this crime. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the e-mail addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion

and control of that account. For the purpose of searching for content demonstrating the actual user(s) of a SUBJECT ACCOUNT, I am requesting a warrant requiring the PROVIDER to turn over all information associated with a SUBJECT ACCOUNT with the date restriction included in Attachment B for review by the search team.

37. Providers of similar services will often keep track of what is referred to as user agent string, which contains information about the type of computer, operating system, and web browser used to access the service. User agent string can include: web requests or HTTP requests (hypertext transfer protocol is the protocol by which many web pages are transmitted between servers and clients or users); logs containing information such as the requestor's IP address, identity and user ID, date and timestamp, request URL or URI (Uniform Resource Locator or Indicator, i.e., a website address), HTTP protocol version, referrer, and similar information; login tracker logs; account management logs; and any other e-mail or social media accounts accessed by or analytics related to the SUBJECT ACCOUNT. These can be used to determine the types of devices used while accessing the SUBJECT ACCOUNT, as well as data related to the user's activity while accessing the SUBJECT ACCOUNT.

38. I have also learned that providers of e-mail and social media services often track the behavior and activities of persons using accounts by using cookies, which are strings of characters and numbers stored on a person's computer on their

web browser. These cookies can often show whether more than one account was accessed by the same computer (and specifically the same web browser), as the provider can recognize that cookie when the same device returns to the service to access an account.

39. In order to identify other accounts used or maintained by the user of a SUBJECT ACCOUNT, the warrant also calls for the PROVIDER to disclose both (1) any cookies associated with the SUBJECT ACCOUNT, i.e., those cookies that were placed on any computers or web browsers (for example, Internet Explorer or Google Chrome) used to access the SUBJECT ACCOUNT, and (2) the identity of any other account in which the same cookie or cookies used to access the SUBJECT ACCOUNT was/were recognized. If in the course of the investigation the digital devices used by the subject(s) of the investigation are found, they can be searched to determine if the cookies recognized by the provider are stored on those devices. The warrant also calls for the PROVIDER to identify any other accounts accessed by any computer or web browser using the same cookies as the SUBJECT ACCOUNT by providing subscriber records and log-in information for those other accounts (but not to provide the contents of communications in those other accounts).

40. Relatedly, the government must be allowed to determine whether other individuals had access to a SUBJECT ACCOUNT. If the government were constrained to review only a small subsection of an account, that small subsection might give the

misleading impression that only a single user had access to the account.

41. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

42. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

43. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for a provider to authenticate information taken from a SUBJECT ACCOUNT as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from a SUBJECT ACCOUNT.

b. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore,

would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

V. CONCLUSION

44. Based on the foregoing, I request that the Court issue the requested warrant.

Emily Tripp, Special Agent
Federal Bureau of
Investigations

Subscribed to and sworn before
me on January ___, 2019.

HONORABLE PAUL L. ABRAMS
UNITED STATES MAGISTRATE JUDGE

Magistrate Case Initiating Documents

2:19-mj-00258 USA v. Search Warrant

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

Notice of Electronic Filing

The following transaction was entered by Lara, Scott on 1/31/2019 at 10:36 AM PST and filed on 1/31/2019

Case Name: USA v. Search Warrant

Case Number: 2:19-mj-00258

Filer: USA

Document Number: 1

Docket Text:

APPLICATION FOR A SEARCH AND SEIZURE WARRANT filed by Plaintiff USA. (Not for Public View pursuant to the E-Government Act of 2002) (Attachments: # (1) Proposed Order) (Attorney Scott Michael Lara added to party USA(pty:pla)) (Lara, Scott)

2:19-mj-00258-1 Notice has been electronically mailed to:

2:19-mj-00258-1 Notice has been delivered by First Class U. S. Mail or by other means **BY THE FILER** to :

The following document(s) are associated with this transaction:

Document description:Main Document

Original filename:N:\Lara, Scott\Search Warrants\2-19-MJ-00258 - Application for 2703 Warrant w Exhibit A .pdf

Electronic document Stamp:

[STAMP cacdStamp_ID=1020290914 [Date=1/31/2019] [FileNumber=27031859-0]
] [6f208609e0fa839762bbed73ef31fd07f51154d3e4fc414054795ffd387d0e29790
48d4b73a4997c010fa3a1f06c279959e7872fff7b479ed05696503880b5bf]]

Document description:Proposed Order

Original filename:N:\Lara, Scott\Search Warrants\2-19-MJ-00258-2703 Warrant .pdf

Electronic document Stamp:

[STAMP cacdStamp_ID=1020290914 [Date=1/31/2019] [FileNumber=27031859-1]
] [71b7829adee318c7634abc2d80bcec019afd168b9d2d445fd84cfbad7b2ea6a2bd6
fa2797de577646b1b0d1e78c9f2752d5c0fa9660c098e7983a05585aa488a]]